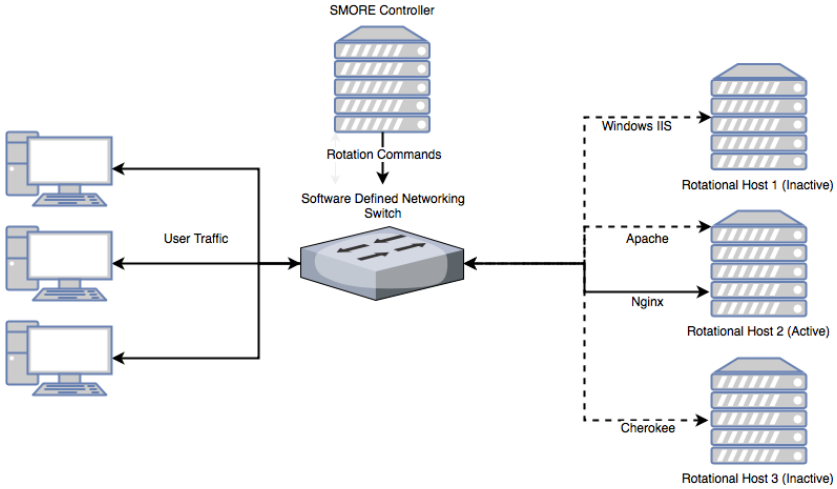
MOVING TARGET DEFENSE (MTD)

SDN MULTIPLE OPERATING SYSTEM ROTATIONAL ENVIRONMENT (SMORE)



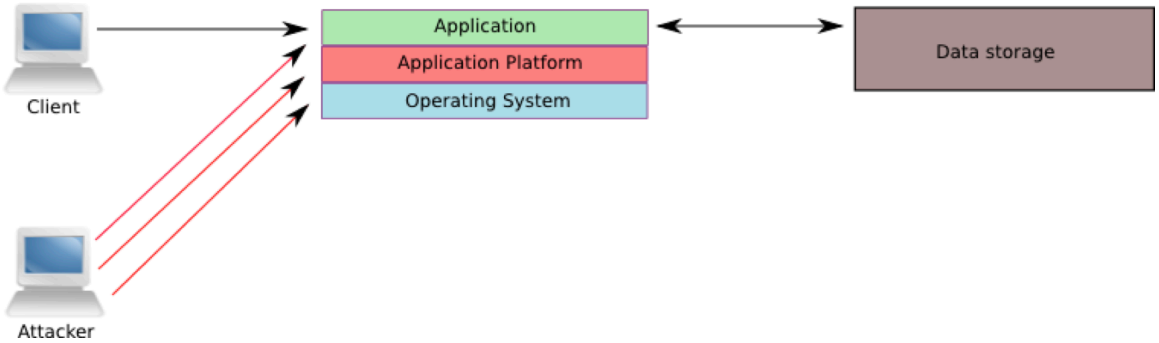
JOSHUA LYLE
Cyber Security Analyst
Argonne National Laboratory

Argonne National Laboratory's work was supported by the U.S. Department of Energy, Office of Science, under contract DE-AC02-06CH11357.

U.S. DEPARTMENT OF ENERGY Argonne National Laboratory is a U.S. Department of Energy laboratory managed by UChicago Argonne, LLC.

ATTACK SURFACE

- In a normal client/server application, the typical client is only concerned about the application itself, where **the attacker's goal is to gain a foothold wherever they can.**
- Since an application developer has a limited amount of control over the platform and operating systems their application runs on, these are natural attack vectors for “hackers” to target.



MOVING TARGET DEFENSE

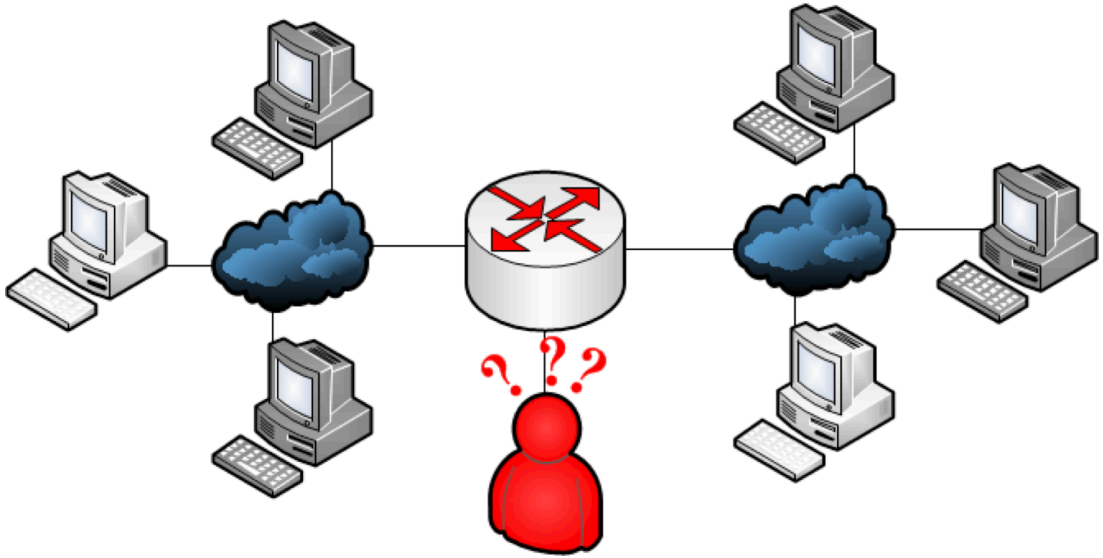
What is it?

- **Based on changing services every *n* seconds**
  Service can be OS, application stack, network device, IP, firewall
- **Effective elimination of Zero Day Exploits**
  Allow vulnerable elements to be removed from danger while maintaining availability
- **Rotation environment allows uptime during normal outage events**
  Quarantining of exploited systems for forensic analysis with zero downtime. Patching, updating, and testing can be done offline with updated systems added post certification with zero downtime.

MOVING TARGET DEFENSE

Increasing Attacker Uncertainty

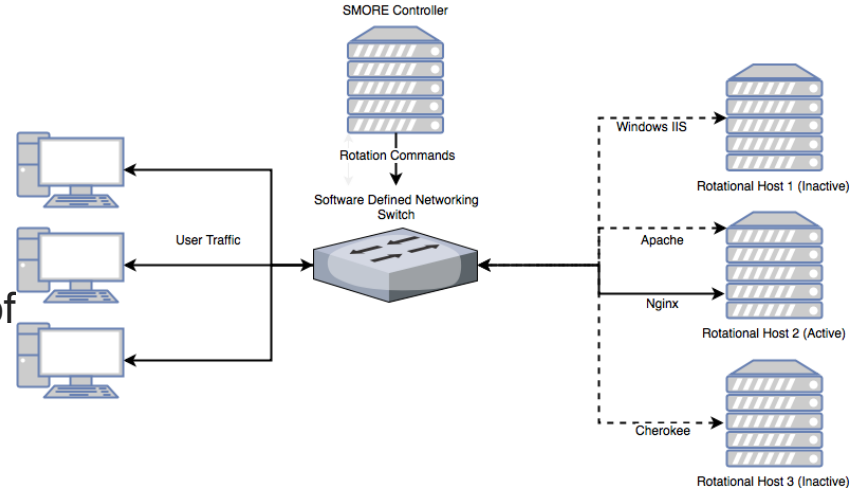
- In attempting to increase attacker uncertainty, we want to eliminate the attacker's advantage in having virtually unlimited time to gather information about a system.



SMORE MOVING TARGET DEFENSE

Operation

- Utilizes software defined networking (SDN) to increase software diversity
  - SDN allows us to manipulate network paths to dynamically select application platforms and operating systems
- SMORE intelligently selects hosts based on responsiveness and possible exploitation
  - Tracks webserver behavior to detect denial of service (DoS) attacks
  - Removes software being affected by DoS attacks to restore application availability
  - Selection criteria which to remove machines from service can easily be expanded



SMORE MOVING TARGET DEFENSE

Application

- Currently being tested with webserver applications
  - Works with any server application without an indefinite connection time
- Setup
  - Requires deploying a web application on multiple platforms (Apache, Nginx, Microsoft IIS) on a multiple operating systems (Windows, Linux, BSD) to provide software diversity
  - Requires setting up an SDN switch connected to SMORE between the internet and the webservers

SMORE MOVING TARGET DEFENSE

Future Work

- Integration with external software to provide rotation management
  - IDS events from Snort/Suricata
  - Performance or error events from Elasticsearch/Prometheus/Splunk
- Automatic removal from rotation on CVE announcement
  - Automatic removal of software from service until it can be patched
- Test with other network services
  - SMTP, DNS, NTP
  - Experiment with SDN flow configurations based on use-case

CONTACT

- Further questions? Interested in partnership?
- Joshua Lyle
  - jlyle@anl.gov
- Nate Evans
  - nevans@anl.gov

THANK YOU

U.S. DEPARTMENT OF ENERGY
Argonne National Laboratory is a U.S. Department of Energy laboratory managed by UChicago Argonne, LLC.

Argonne NATIONAL LABORATORY